IJBPAS, February, 2023, 12(2): 834-846

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

AN OVERVIEW ON CYBERSECURITY IN PACEMAKERS

YAMINI DIVYA TEJA. G*, KOUSHIK Y AND RAMA RAO N

Dept. of Pharmaceutical Regulatory Affairs, Chalapathi Institute of Pharmaceutical Sciences,

Guntur, Andhra Pradesh, India

***Corresponding Author: Guntupalli Yamini DivyaTeja: E Mail: yaminiguntupalli24101998@gmail.com**

Received 8th April 2022; Revised 3rd May 2022; Accepted 25th July 2022; Available online 1st Feb. 2023

https://doi.org/10.31032/IJBPAS/2023/12.2.6868

ABSTRACT

As computer networks became more connected, medical devices became more prone to cyber-attacks. To prevent medical devices from cyber threats, recognizing the complexities and listing all the technical vulnerabilities is crucial. Protection of medical devices from cyber threats is not just a technical issue but a difficult problem to solve. Identification of vulnerabilities, as well as a review of the aspects that influence to a potentially dangerous environment, is critical for determining why the risk persists and determining the best course of action. When patient safety concerns addressed, a systematic approach is essential for such multidimensional challenges. Along with correlated and dedicated perspective it is vital to know technical controls, supremacy, flexible measures, secure reporting, experts, and modernized regulations as well as standards as patient wellbeing is in threat. To maintain patient's safety and medical device efficacy the regulatory authorities maintain some standards and the manufacturers are mandated to demonstrate that their devices are following all the guidelines by submitting the required documents to respective regulatory authority. However a lot of work has been done in this area, there is still opportunity for more research and development. Hardware advancements will also play a significant role, as computing units get more powerful and storage capacity increases as device sizes decrease.

Keywords: Cyberthreats, manufacturers, medical device, healthcare providers, ulnerabilities

INTRODUCTION:

Kevin Fu, acting director of medical device cybersecurity at the FDA's Center for Devices and Radiological Health (CDRH), stated that medical devices and healthcare facility networks are being interrupted by ransomware attacks placing patient's health at risk **[1]**.

Cardiovascular Disease (CVD) is the world largest leading cause of mortality, with an estimated 23.6 million deaths by 2030, according to the World Health Organization (WHO) **[2]**. It is like a double-edged sword while approaching to mobile health (mHealth) technologies and other networked medical devices because they play a key role in health care along with acting as a medium to reveal patients and health care providers leading to expose them to safety and cybersecurity risks **[3]**. Patients with moderate to severe heart failure can use medical devices like Pacemakers, Implantable like Cardiac Resynchronization (CRT-P) and Pulse Generator.

An implantable pacemaker pulse generator is a device with a power supply and electronic circuits that acts as a substitute to produce a periodic electrical pulse for stimulating the heat device so as to correct both intermittent and continuous disorders related to cardiac rhythm caused by the heart's essential pacing system **[3]**.

1. Types of Pacemakers:

Based on the symptoms and heart condition pacemaker used may vary.

1.1 Single-chamber pacemaker:

Using one lead, heart's one chamber is linked to the pulse generator **[4]**. These type of pacemakers control pacing of heart beat by connecting right ventricle with lead or if required based on symptoms we can connect to right atrium based on patients requirements **(Figure 1)**.

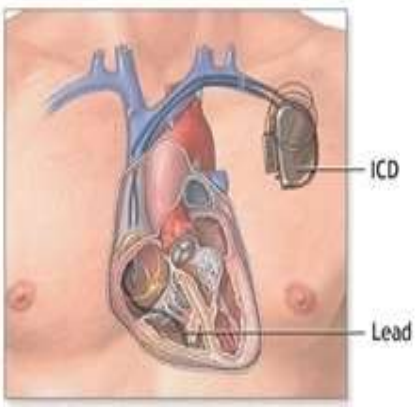

Figure 1: Single-chamber pacemaker

1.2 Dual-chamber pacemaker:

Right atrium and ventricle of heart are associated to the device by two leads **(Figure 2)**.

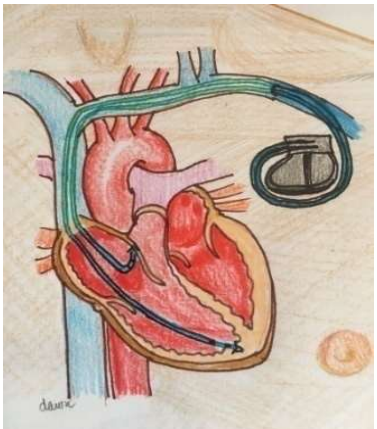

Figure 2: Dual-chamber pacemaker

1.3 Biventricular pacemaker:

It resynchronizes the ventricles pumping action and named as cardiac resynchronization therapy pacing device (CRT-P) **[4]**. Biventricular pacemaker is associated to both ventricles and to the right atrium by using three leads. This biventricular pacemaker helps in treating arrhythmias due to advanced cardiac failure **(Figure 3)**.

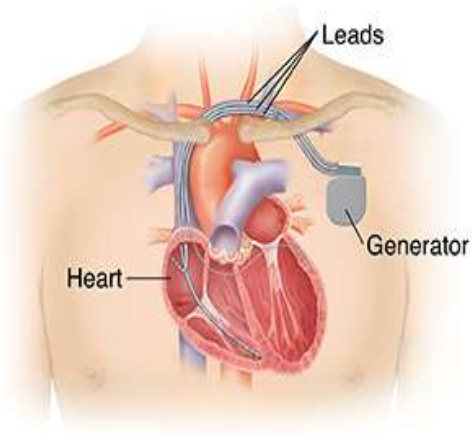

Figure 3: Biventricular pacemaker

2. PREVENTION OF CYBERSECURITY RISKS:

To ensure safety healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) must take necessary steps. Placing appropriate mitigations to maintain patient's security and ensuring device performance are the responsibilities of both HDOs and MDMs **[5]**.

MDMs are liable for staying diligent in recognizing hazards and risks linked with their products, including cybersecurity concerns.

Health care delivery organizations (HDOs): HDOs conduct network protection and security assessments for healthcare systems **[5]**.

Defining two "tiers" of devices according to their cybersecurity risk:

Tier 1 "high Cybersecurity Risk": Criteria for a medical device to be as a tier 1

a. Capability of connecting to devices **[5]**
b. A cybersecurity threat impacting the device might cause several people to be harmed in the same way.

Examples: Implantable cardioverter defibrillator (ICDs), Pacemakers, left ventricular assist devices (LVADs), Brain stimulators, Neurostimulators, Dialysis devices, Insulin pumps and Infusion **[6]**,

Tier 2 "Typical/ Normal Cybersecurity Risk": A medical device that does not met the Tier 1 device standards.

CYBERSECURITYFRAMEWORK:

Cybersecurity frameworks core function is to guide the manufacturers of medical device in cybersecurity activities. This framework involves **(Figure 4)**.

A. Identify and Protect:

To ensure that the security measures are appropriate for the intended users, manufacturers should carefully assess the balance between cybersecurity precautions

and the usability of the device in its intended context of use (e.g., home usage vs. health care facility use). For instance, security controls should not obstruct access to implantable medical devices (IMD) that is intended to utilize in any emergency.

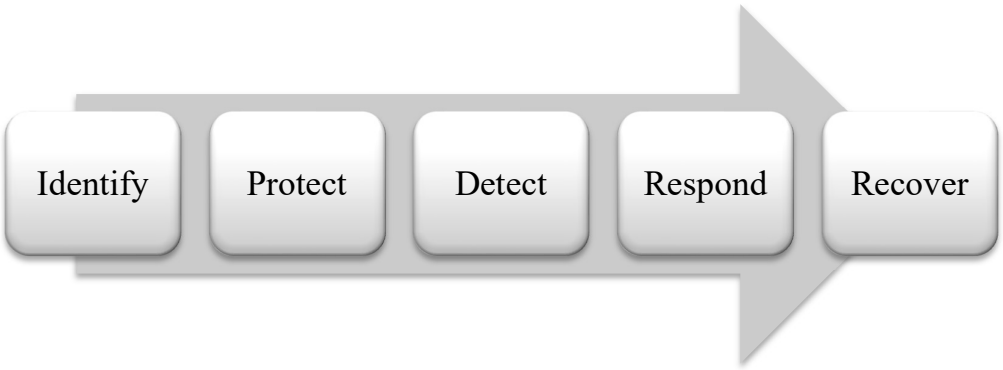

Figure 4: Framework for Cybersecurity

Medical device makers should justify the security functionalities they choose for their devices in their premarket submissions, according to the FDA. Some security functions to be considered for the protection of IMD:

Providing access to Trusted Individual Only

- Users' authentication (e.g., biometric, password and user ID, smartcard) is used to limit device access.
- Where appropriate for the usage scenario, employ automatic timed mechanisms to end sessions within the system.
- Use multilayer authorization architecture to differentiate rights depending on user role (e.g. caregiver, system administrator) or device role where appropriate.
- Use adequate authentication (e.g., multi-factor authentication to grant service technicians, system administrators, and maintenance workers privileged device access);
- Limit unauthorized access to a system used for privileged device access in public, and don't use "hardcoded" passwords or words that are easily remembered. (i.e. passwords that are same for every device, impossible to change, and subject to public exposure). It means the stronger the password the more safer and secure the device **[6]**.
- Provide physical locks on devices and their communication ports as needed to prevent tampering;

Before allowing software or hardware upgrades, such as those impacting the operating system, apps, and anti-malware,

need user authentication or other necessary safeguards.

Ensure Trusted Content

- Only allow authorized code to update software or firmware. Code signature verification is one authentication approach that manufacturers may investigate;
- Use systematic methods for authorized users to get version-identifiable software and firmware from the manufacturer;
- Determine the device's capacity to securely transport data to and from it, and utilize encryption mechanisms as needed.

B. DETECT, RESPOND, RECOVER:

- Incorporate features that allow security violations to be detected, identified, tracked, timed, and responded to during regular use.
- Develop and disseminate information to end users on the proper course of action to be taken when cybersecurity incidents occur;
- Device features must be implemented to safeguard key functionality when device's security is compromised;
- Provide mechanisms for an authorized privileged user to save and retrieve device settings.

Manufacturers may choose to use a different strategy or approach if they can justify it **[6]**.

CYBER SECURITY DOCUMENTATION FOR DEVICES OF TIER 1 CATEGORY TO BE SUBMITTED TO USFDA:

Premarket submission:

Specifically, FDA recommends the manufacturers to include documentation related to design characteristics management of risk along with labeling to demonstrate a risk-based approach that includes design characteristics and cybersecurity level required for flexibility of device **[6]**.

Design Documentation:

1. Documentation for Tier 1 devices :
   a. establish and defend Device Assets and working
   b. Device designed to discover cybersecurity events in a very timely fashion
2. System Diagrams sufficiently elaborated to allow associate understanding of however the precise device style components area unit incorporated into a system-level and holistic image. Analysis of the whole system is critical to know the manufacturer's threat model and also the device at intervals the larger system. System diagrams ought to include:

a) Network, flow, design, and state diagrams.
b) The components, interfaces, communication pathways, assets, network ports, and protocols.
c) Controls and authentication mechanisms for every act plus or element of the system together with internet sites, servers, cloud stores, practical systems, etc.
d) Roles and responsibilities of users who interact with these assets or communication channels
e) Use of cryptographical strategies ought to embrace descriptions of the strategy used and also the kind and level of cryptographical key usage and their kind of use throughout your system (one-time use, key length, the quality used, bilaterally symmetric or otherwise, etc.). Descriptions ought to additionally embrace details of crypto graphical protection for microcode and computer code updates. Descriptions have to include information of cryptographic protection for firmware and software updates.

3. An outline describing the look options that let valid computer code updates and patches as required throughout the life cycle of the medical device to still guarantee its safety and effectiveness **[7]**.

Risk Management Documentation:

Design is linked to clinical hazards, threat models, mitigations, and testing in risk assessments. It's necessary to determine secure style design specified risk will be adequately managed. A security risk management report could be a comprehensive approach that considers each security and safety risk analysis in an exceedingly important manner. It provides analysis outline, assessment, and mitigation activities that assure a tool is fairly secure. The subsequent recommendations related to management report of a trustworthy device:

1. A framework threat model that considers system-level risks, including but not limited to risks related to the supply chain (e.g., to ensure the device remains free from malware), design, production, and preparation.
2. A selected list of all cybersecurity risks that were thought-about within the style of your device. We tend to advocate providing descriptions of risk that leverage an analysis of exploitability to explain probability rather than likelihood. If numerical possibilities are provided, we tend to advocate providing extra data that

explains however the likelihood was calculated **[7]**.

3. All cybersecurity safeguards that were set up for your device are listed here, along with their justifications. This could hold all threat mitigations and style issues bearing on intended and accidental cybersecurity risks related to your device, including:
    a. An inventory of verifiable function/subsystem necessities associated with access management, encryption/decryption, firewalls, intrusion detection/prevention, antivirus packages, etc.
    b. A listing of verifiable of security necessities impacting alternative practicality, data, and interface necessities.
4. An outline of analysis that was prepared to create the capability of security risk controls and cyber activities (e.g., security effectiveness in implementing the required security policy, performance for needed traffic conditions, stability and responsibility as appropriate). Take a look at reports ought to include:
    a. Testing of device performance
    b. Evidence of security effectiveness of third-party OTS software in the system
    c. Fixed and vibrant code analysis as well as analysis for credentials that are "hard-coded", default, easily-founded, and simply compromised.
    d. Vulnerability scanning
    e. Hardness analysis
    f. edge analysis
    g. transmission Testing
    h. External (Third party) test reports
5. A traceability matrix that links your actual cybersecurity and risks that were considered in your security risk and hazard analysis should be connected.
6. A Cybersecurity bill of materials (CBOM) must be cross referenced with the National Vulnerability Database (NVD) or with similarly recognized vulnerability databases.

Provide norms for addressing identified vulnerabilities and a justification for not addressing other better-known vulnerabilities, according to final regulations of medical devices cybersecurity for post market management by FDA **[7]**.

Recommended Content to incorporate in premarket approval (PMA) Devices Periodic Reports:

Data about cybersecurity vulnerabilities, along with device changes and compensating controls implemented with respect to the current data, must be reported

to FDA in an exceedingly periodic (annual) report for PMA devices with periodic reports according to 21 CFR 814.84 **[8]**. It is suggested that the following data be provided for device changes with compensating controls:

a. a short description of the vulnerability prompting the modification together with however the firm became alert to the vulnerability;
b. An outline and conclusions of risk assessment together with whether the danger to patient was controlled or uncontrolled;
c. an outline of the change(s) created, together with a comparison to the antecedents approved version of the device;
d. The principle for creating the change;
e. relevance different submissions/devices that were changed in response to the present same vulnerability;
f. Identification of event(s) associated with the rationale/reason for the modification (e.g., MDR number(s), recall number);
g. Unique Device Identification (UDI) ought to be enclosed, if available;
h. A link to associate degree ICS-CERT or different government or ISAO alert (https://icscert.us-cert.gov/advisories), if applicable;
i. All distributed client notifications;
j. The date and name of the ISAO to that the vulnerability was rumored, if any; and
k. Relevance different relevant submission (PMA Supplement, 30-Day Notice, 806 report, etc.), if any, or the scientific and/or restrictive basis for last that the modification failed to need a submission/report **[8]**.

Resolution to Secure IMDs

1) **Close-Range Communication:** IMDs upon communication with external devices expose themselves to attacks. Radio-frequency identification (RFID) contains tag to connect the IMD and to read the information. The tag is roofed with liquid seal. It contains data of concerned patient and the medical practitioner solely can access the device. VeriChip is an implantable RFID medical device that consists of a chip tag implanted in a human body that contains a novel ID range linked to information about the patient's medical history, allergies, medications, and contact information. The reader will access the tags' data from 10 to 15 cm. **Figure 5** represents the implantable

tag and information communication. The communication between the IMD and the information ought to be secured over the three channels: the channel between the tag and also the reader and also the channel between the reader and also the information over the internet. Moosavi *et al*. Bestowed a brand-new protocol which might secure the channel between the tag and also the reader victimization elliptic curve cryptography.

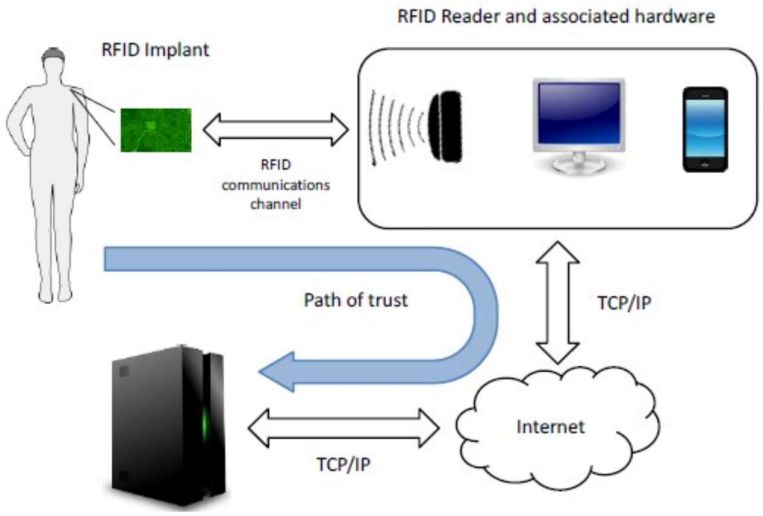

Figure 5: Implantable tag and communication of information

2) **Cryptography**: Cryptographic solutions for securing IMDs have been developing. Two types of encryption are available, symmetric-key cryptography, where communication entities share a confidential key, and public-key cryptography, in which one is public and the second is a secret. For instance presents a solution based on public-key cryptography, but the major drawback lies in the high energy consumption of this solution. Hosseini-Khayat designed a device that can be used with ultra-low power ASIC chips by using a symmetric-key of light weight. Zhend Designed technique which require a shared key formed by ECG signal. Data compression technology is used in decreasing the power usage.
3) **External Devices:** Denning along with his team placed a proposal which includes using external devices. Operation of a working

device is shown in **Figure 6**. An external device receives signals rather than being sent directly to the IMD. The entire incoming request are controlled and managed by external device for the protection of IMDs from various attacks.

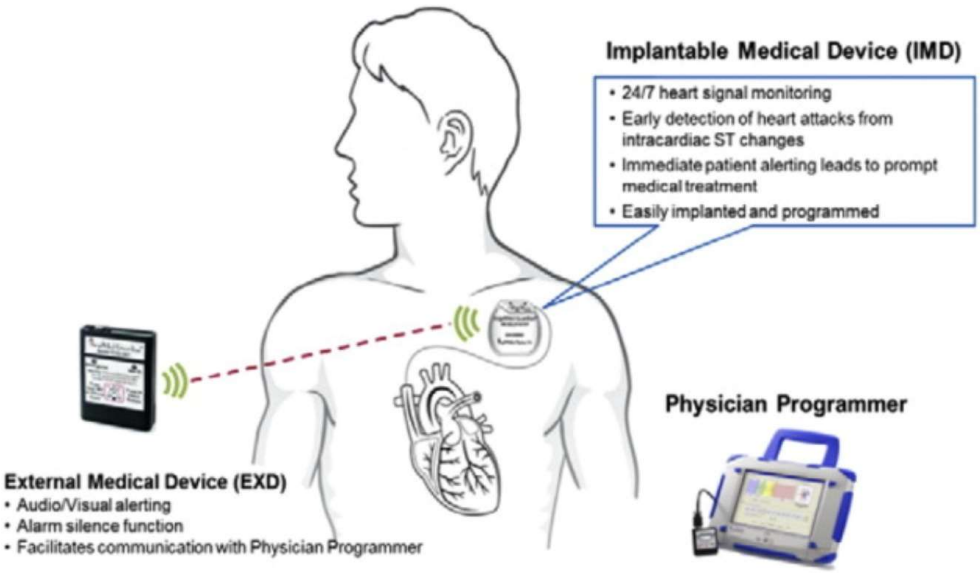

Figure 6: Using External Medical Devices

The external device is reversible and has fewer restrictions on the dimensions than the IMD. Just in case of urgency, the medical workers will take away the external device and communicate directly with the IMD. A downside of this solution is that the patient should always be round the external device. This solution is additionally appropriate just in case when the IMD is already in the patient body and security has to be additional added afterwards **[8]**.

4) **Biometric Access:** Using biometrics like fingerprints, iris, and voice to access the IMD, will mitigate the imperative access restriction. Hei and Du projected a two-level access system. The primary level uses the patient's fingerprints, iris, color, and height as biometry, whereas the second level uses an efficient iris verification process. In emergencies, the medical employees will use the patient's biometry to access the information, that doesn't need a lot of responsiveness from the patient. It additionally doesn't need the patient to remember any passwords or carry authentication tokens **[9]**.

5) **Battery Constraint Mitigation**: The battery-depleting attack causes a severe threat to IMDs since a battery replacement typically wants a surgical intervention. A part from reducing the battery consumption by using lightweight coding and external devices, alternative approaches are often used, like reposing the battery constraints by creating the implant wirelessly rechargeable or strap up K.E. from the human. A huge work should be done in the technical view, and clinically to make use of this way **[9]**.

CONCLUSION:

Medical devices are becoming increasingly connected to hospital networks, Internet, and other medical devices to provide features that improve health care and the ability of health care providers to treat patients. These same characteristics raise the possibility of cyber-threats. Medical devices, like other computer systems, are vulnerable to security breaches, which could jeopardize the device's functionality and safety. We emphasized the significance of considering safety as a primary consideration in the improvement of IMDs. Many current IMD vulnerabilities, design limitations that prevent IMD protection and potential ways to solve have been described. As the technology advances the regulatory authority updated their guidelines for improving and ensuring the quality, safety, and efficacy of medical devices. Even though huge work is being done in the field, there is still room for research and improvement. Advances in network communications and the Body Area Network (BAN) can prove to be beneficial in protecting IMD. Stronger and faster encryptions can be developed and employed to secure the data communicated over the network. Wireless rechargeable batteries will revolutionize many areas, including medical applications. Advances in hardware technologies will also play an important role, as the computation devices become more powerful and storage capacity becomes larger, while devices size get smaller.

Acknowledgment: I would like thank our staff of CLPT IPR and CLPT IQAC cells of Chalapathi Institute of Pharmaceutical Sciences, Guntur.

No financial support

No conflict of Interest

REFERENCES:

[1] Medtechdive (2021)Ransom ware attacks put availability of medical devices at risk: FDA cyber chief[online] https://www.medtechdive.com/news/cyber-attacks-security-medical-devices-kevin-fu-advamed/607483/?__cf_chl_captcha

_tk__=pmd_WQLaXLh29z46d_ThOegvNMgjCQM.yIuTV8uCDjwkgrg-1635746760-0-gqNtZGzNA1CjcnBszQsl

[2] Diana Moses and Deisy C. (2015). A survey of data mining algorithms used in cardiovascular disease diagnosis from multi-lead ECG data. Kuwait Journal Of Science, 42(2): 206-235,

[3] Russell L. Jones and Sheryl Coughlin (2021) Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives, October 2021 [online]. available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-networked-medical-device-11102014.pdf,

[4] Stanford health care (2021) Types of pacemakers, October 2021[online] available at: https://stanfordhealthcare.org/medical-treatments/p/pacemaker/types.html

[5] United States food and Drug Administration (FDA) (2022) Cybersecurity January 2022 [online]. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#safety,

[6] United States food and Drug Administration (FDA) (2022) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff [online]. https://www.fda.gov/media/86174/download

[7] United States food and Drug Administration (FDA) (2022) Content of Premarket Submissions for Management of Cybersecurity in Medical devices [online]. https://www.fda.gov/media/119933/download, accessed October 2021

[8] United States food and Drug Administration (FDA) (2022) Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff[online]. https://www.fda.gov/files/medical%20devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf, accessed October 2021.

[9] Tabassum Aliya, Safi Zeineb, AlKhater Wadha & Shikfa Abdullatif. (2018). Cybersecurity Issues in Implanted Medical Devices.

1-9.10.1109/COMAPP.2018.8460454.

[10] U.S. food & drug administration product classification. (FDA) (2021)[online] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/classification.cfm?id=1074,accessed

[11] Med tech intelligence, (2021) [online] available at: https://www.medtechintelligence.com/column/implanted-medical-devices-and-vulnerabilities-to-hackers.

[12] U.S. food & drug administration product classification. (2021) [online] Available at: https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

[13] Raising the Bar for Medical Device Cybersecurity. (2021) [online] Available at: https://www.dicardiology.com/article/raising-bar-medical-device-cyber-security

[14] Cybersecurity of medical devices. (2021) [online] Available at https://www.bsigroup.com/LocalFiles/ENAU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf

[15] Williams, Patricia & Woodward, Andrew. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical devices (Auckland, N.Z.). 8. 305-16. 10.2147/MDER.S50048.

[16] Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, Fu K, *et al*. (2012) Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. PLOS ONE 7(7): e40200.

[17] Mary Carol Day, Christopher Young. (2012). This is your heart speaking. Call 911. Ergonomics in Design: The Quarterly of Human Factors Applications, 20 (2); 4-12